cybeRéponse RFC2350

Version 2.0

RÉSUMÉ

Ce document contient une description de cybeRéponse, le CSIRT du Centre Val de Loire, tel que recommandé par la RFC2350. Il présente des informations relatives à l'équipe, aux services proposés et aux moyens de contacter cybeRéponse, CSIRT de la region Centre Val de Loire .

CSIRT | CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ DE LA REGION CENTRE VAL DE LOIRE

Table des matières

I. AVANT-PROPOS....3
II. LISTE DE DIFFUSION....3
III. HISTORIQUE DES VERSIONS....3
IV. VALIDATION DU DOCUMENT....3
V. RFC2350....4
1. À propos du document....4
a. Date de la dernière mise à jour....4
b. Liste de distribution pour les modifications....4
c. Où trouver ce document....4
d. Authenticité du document....4
e. Identification du document....4
2. Informations de contact....4
a. Nom de la structure....4
b. Adresse....4
c. Zone horaire....4
d. Numéros de téléphone....4
e. Numéro de Fax....5
f. Autres moyens de communication....5
g. Adresse e-Mail....5
h. Clé publique et informations liées au chiffrement....6
i. Membres de l'équipe....6
j. Autres informations....6
k. Contact....6
3. Charte....7
a. Ordre de mission....7
b. Bénéficiaires....7
c. Affiliations....7
d. Autorité....7
4. Politiques....7
a. Types d'incidents et niveau d'intervention....7
b. Coopération, interaction et partage d'information....8
c. Communication et authentification....8
5. Services....8

a. Réponse aux incidents....8
b. Activités proactives....9
6. Formulaire de notification d'incident....9
7. Décharge de responsabilité....9

I. AVANT-PROPOS

Ce document respecte les définitions et les usages du standard TLP[1] version 2.0 [Traffic Light Protocol] du FIRST[2] dont Olivier Caleff siège au conseil d'administration pour la France. Ce document est actuellement labellisé par son auteur **TLP:CLEAR** .

II. LISTE DE DIFFUSION

LISTE DE DIFFUSION				
Entité	Nom	Motif de diffusion		
		Information	Avis	Mise en œuvre

III. HISTORIQUE DES VERSIONS

HISTORIQUE DES VERSIONS			
Version	Date	Auteur	Objet
V 0.1	11/08/2022	Victor-Emmanuel de SA	Création
V 1.1	12/11/2022	Victor-Emmanuel de SA	Ajouts et compléments
V 1.2	09/03/2023	Victor-Emmanuel de SA	Modifications
V 2.0	20/02/2025	Yahya SY	Mise à jour et modifications

IV. VALIDATION DU DOCUMENT

VALIDATION			
Entité	Nom	Date	Visa / Observations

[1] https://www.first.org/tlp/
[2] https://www.first.org/

V. RFC2350

1. À propos du document

Ce document contient une description de cybeRéponse tel que recommandé par la RFC2350. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter cybeRéponse.

a. Date de la dernière mise à jour

Ceci est la version 2.0 de ce document, éditée le 20 février 2025.

b. Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants : https://www.cybereponse.fr

c. Où trouver ce document

Ce document peut être trouvé sur le site de cybeRéponse : https://www. cybereponse.fr

d. Authenticité du document

Ce document a été signé à l'aide de la clé PGP de cybeRéponse.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet de cybeRéponse à l'adresse suivante : https://www. cybereponse.fr

e. Identification du document

Titre : cybeRéponse ORG v2.0_RFC2350_02-25

Version : 2.0

Date de mise à jour : 20 février 2025

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

2. Informations de contact

a. Nom de la structure

Nom court : cybeRéponse

Nom complet : cybeRéponse | Centre de Réponse aux Incidents de Cybersécurité de la Région Centre-Val de Loire

b. Adresse

cybeRéponse CSIRT Centre-Val de Loire

GIP-RECIA

Bâtiment F1 | BP 36009 | 45060 Orléans Cedex 02

c. Zone horaire

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

d. Numéros de téléphone

Le numéro d'urgence cyber est le 0 805 69 15 05. C'est un numéro vert gratuit.

Le numéro d'information génerale est le 02 19 230 466.

e. Numéro de Fax

Aucun à ce jour.

f. Autres moyens de communication

Aucun à ce jour.

g. Adresse e-Mail

contact@cybereponse.fr

h. Clé publique et informations liées au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec cybeRéponse.

Identifiant utilisateur : cybeRéponse

Identifiant de la clé : cyber@cybereponse.fr

Empreinte : 123A B45Z

La clé PGP publique est disponible à cette adresse : https://www. cybereponse.fr ainsi que sur les principaux serveurs de clés PGP :

- https://pgp.circl.lu
- https://pgp.mit.edu
- https://keys.openpgp.org
- https://keyserver.ubuntu.com
- https://keyserver.pgp.com

i. Membres de l'équipe

L'équipe est constituée de plusieurs membres :

- Un responsable du CSIRT cybeRéponse
- Un responsable infrastructure
- Un responsable relation prestataires Cyber
- Plusieurs analystes de niveau 1.

j. Autres informations

Aucune à ce jour.

k. Contact

cybeRéponse est disponible durant les heures ouvrées, soit de 09h00 à 12h30 et de 13h30 à 17h00, du lundi au vendredi [hors jours fériés].

Pour joindre cybeRéponse, le moyen de communication privilégié est le numéro d'information générale est le 02 19 230 466 et, en seconde intention, par courriel à l'adresse **contact@cybereponse.fr**.

En cas d'urgence cyber, le numéro vert gratuit est le 0 805 69 15 05.

En dehors de ces heures les adhérents peuvent signaler leur incident auprès de l'Agence Nationale de la sécurité des Systèmes d'Information [ANSSI] dont les coordonnées figurent à l'adresse suivante : http://www.cert.ssi.gouv.fr/contact/, ou bien auprès du site de : www.cybermalveillance.gouv.fr

Afin d'assurer l'intégrité et la confidentialité des échanges, nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe 2.h Clé publique et informations liées au chiffrement.

3. Charte

a. Ordre de mission

cybeRéponse est l'équipe de réponse aux incidents de sécurité informatique de la région Centre-Val de Loire. Son objectif est d'apporter une assistance aux organisations de son territoire [décrites dans le paragraphe 3.b Bénéficiaires] pour répondre aux incidents de cybersécurité auxquels elles font face.

Les missions de cybeRéponse sont :

- Accompagner les bénéficiaires du dispositif [3.b] victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région
- Assurer une veille à partir de l'écosystème cybersécurité régional et national sur les menaces et les vulnérabilités ;
- Alerter les bénéficiaires de ces menaces et vulnérabilités ;
- Contribuer à la sensibilisation des entreprises de la région de manière permanente en relayant les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.

b. Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement de cybeRéponse sont les organisations localisées sur le territoire de la région Centre-Val de Loire, comprenant notamment :

- Les PME | PMI ;
- Les ETI ;
- Les collectivités territoriales et les établissements publiques associés de plus de 5000 habitants ;
- Les associations employeuses.

c. Affiliations

cybeRéponse est affilié à la Région Centre-Val de Loire , au GIP-RECIA et de l'Agence de développement économique Dev'Up de la Région Centre-Val de Loire

d. Autorité

cybeRéponse réalise ses activités sous l'autorité du GIP-RECIA et de l'Agence de développement économique Dev'Up, dont la Région Centre-Val de Loire est membre fondateur.

4. Politiques

a. Types d'incidents et niveau d'intervention

Le périmètre d'action de cybeRéponse couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe 3.b Bénéficiaires.

Les missions principales de cybeRéponse sont :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;

- Rediriger ses bénéficiaires vers des prestataires régionaux pour la remédiation de l'incident ;
- Agir en coordinateur entre le CERT-FR, les prestataires régionaux, les services de Police et de Gendarmerie et les bénéficiaires ;
- Consolider les statistiques d'incidentologie à l'échelle régionale.

cybeRéponse est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses bénéficiaires. En fonction de la nature de l'incident, cybeRéponse propose une liste de prestataire en Cybersécurité, susceptible d'aider l'entreprise dans la résolution de l'incident. Un suivi de la résolution de l'incident est assuré afin de statistiques et de capitalisation, et pour améliorer les capacités de diagnostic.

Le niveau de support offert par cybeRéponse peut varier en fonction du type d'incident, de sa criticité, et des ressources disponibles pour le prendre en charge. Dans le cas où l'incident concerne une structure non bénéficiaire, celle-ci pourra être redirigée vers d'autres centres de réponse à incident.

b. Coopération, interaction et partage d'information

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée : le bénéficiaire.

cybeRéponse peut être amené à communiquer des informations aux autres CSIRT régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées à un CSIRT sectoriel [santé, maritime…] à des fins de capitalisation des incidents propres au secteur concerné.

La diffusion d'information sera traitée en accord avec le protocole TLPv2 défini par le FIRST [https://www.first.org/tlp].

c. Communication et authentification

cybeRéponse conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

Les informations non confidentielles ou peu sensibles peuvent être transmises via des courriels non chiffrés.

5. Services

a. Réponse aux incidents

L'activité principale de cybeRéponse est de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents.

En particulier, il propose les services détaillés dans les paragraphes suivants :

- Triage

Récupération du signalement et prise de contact avec le déclarant ;
Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident ;
Détermination de la sévérité de l'incident [son impact] et de son périmètre [e.g. nombre de machines affectés] ;
Catégorisation de l'incident.

- Coordination

Identification du meilleur partenaire au sein du dispositif national de réponse aux incidents pour accompagner le demandeur ;
Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident.

Notamment, mais de manière non exhaustive :

- A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
- A la Commission Nationale de l'Informatique et des Libertés [CNIL] en cas de violation de données à caractère personnel.

- Résolution

Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident ;
Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident ;
Suivi des phases de résolution et de remédiation.

b. Activités proactives

cybeRéponse pourra aussi proposer des services proactifs à ses bénéficiaires adhérents, notamment des services de veille ; des analyses de menaces ou encore un bulletin de veille à destination de ses adhérents abonnés.

6. Formulaire de notification d'incident

Aucun formulaire de notification n'est actuellement disponible en ligne.

Nous encourageons nos bénéficiaires à déclarer les incidents par téléphone via le numéro d'urgence cyber 0 805 69 15 05

7. Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, cybeRéponse n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.